All except I

REPORT BY UFFZ. KARRENBERG ON THE

BANDWURM

Attached is a complete translation of a report written at our request by Uffz. KARRENBERG, of OKH Gen. der N.A., Gruppe VI on the Russian "BANDWURM" system. The report was written at CSDIC (UK) in September 1945.

Previous reports by the KARRENBERG party have been issued as TICOM/I-30, 149, 157, 166, 167 and 168.

TICOM

2nd December, 1945

No. of pages 25.

Copy No. 15

DISTRIBUTION

British

1. D.D.I.
2. H.C.G.
3. D.D.(N.S.)
4. D.D.(M.W.)
5. D.D.(A.S.)
6. C.C.R.
7. Cdr. Tandy
8. Major Morgan

U.S.

9-12. Op-20-G (4) (via Lt.Cdr.Manson)
13. G-2 (via Lt. Col. Hilles)
14-17. A.S.A. (4) (via Capt. Collins)
18. Director, S.I.D. USFET
19. Col. Kunkel, USAAFE

TICOM

20. Chairman
21-23. S.A.C. (3)
24. Cdr. Bacon
25. Lt. Cdr. Manson
26. Major Cowan
27. Capt. Collins
28-31. Ticom Files (4)

Additional

32. D.D.(A)
33-35. Mr. Pritchard (3)
36. Mr. Twinn
37. Mr. Bonsall for U.S.I.S.

FUNDAMENTAL REMARKS ON THE "BANDWURM"

ENCIPHERING SYSTEM

The "Bandwurm" is an endless, non-repeating column substitution. Encipherment is effected mechanically by impulses according to the five impulses of the BAUDOT alphabet. According to the setting, the cipher teleprinter attachments modifies the individual out-going impulses , i.e. with positive setting of the cipher T/P attachment, each positive impulse becomes negative and vice versa. With negative setting, the positive impulses remains positive, the negative negative.

Outgoing impulse	+ −	+ −
Cipher T/P attachment	+ +	− −
Transmitted impulse	− +	+ −

Thus the letter A, for instance, enciphered with the letter П would produce the letter H.

A	+	−	−	−	−
П	+	+	+	+	+
H	−	+	+	+	+

For each letter, therefore, there are 32 possibilities of encipherment (see table on page following).

The cipher T/P attachment has two settings, one LARGE setting and one SMALL setting. The large setting

ПОШЛИ БОЛЬШИЕ

always gives a simple substitution, that is to say encipherment always takes place with the same letter (the wheels of the cipher T/P attachment do not move). With the small setting

ПОШЛИ МАЛЫЕ

the substitution system changes from letter to letter - probably by movement of the wheels of the cipher T/P attachment - and an endless column substitution is produced.

The system can be broken when messages are received on the same key, and the key itself has been obtained from them.

(b)(1)
(b)(3)-P.L. 86-36

[redacted] the traffic of the whole network must be covered all the time and very carefully. It is not always easy to recognise messages [redacted] They occur:

1) In traffic between the reciprocal stations of a link

[redacted] This appears from the "large" setting, as well as from the announcement of key and table.

Example:

СТАВИМ В ОБЕ I7

Or:

ПОШЛИ В ОБЕ I7

Contact traffic of the T/P operators should also be watched. This often gives the setting away, and constantly allows important conclusions to be drawn regarding key-identity of the messages.

Often the external picture presented by the messages is such that it is only after lengthy investigation that they can be recognised [redacted] For that reason, the traffic must always be examined most carefully.

If evidence of key-identity does not emerge from the setting announcement or from contact traffic, [redacted] when traffic is running smoothly, and on days when a lot of material is transmitted, one can count on key-identity being given away by repeats. [redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

It requires a very practised eye to recognise such cases among thousands of letters.

Often the use of the letter shift key before the start of a new message or a new paragraph also causes repeats to be formed. Such repeats are the most easily recognised.

2) In messages of one and the same station:

a) In repeats sent at the request of the reciprocal station (watch reciprocal traffic!). [redacted] The contact traffic which comes first, enciphered on the "largo" setting, can also occassionally facilitate recognition of these repeats.

(b)(1)
(b)(3)-P.L. 86-36

Example:

ПОШЛИ БЛШ - МУМУМУМУМУМУМУМУМУ

Repeat:

СТАВЛЮ СНОВА ТВОЮ БЛШ -/- МУМУМУМУМУМУМУМУ

b) When the reciprocal station has had reception, the same setting is sometimes used three to four times. In this case, enciphered contact traffic can be reckoned with. The text of this might be as follows:

ТТТТТТТТТТТТТТТТТТТТТТТТТТТ

-/-/-/-/-/-/-/-/-/-/-/- ././/./././././.

ТАМЛИ - ТАМЛИ ТМЛ ТМЛ ТМЛ ТМЛ ТМ ТМ ТМ

ТГСЛНД А. I 123 ТГСЛНД ТГСЛДН

IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

ЗДЕСЬ ЗДЕСЬ ЗДС ЗДС ЗДС ЗДС

НУС КАК

РОБИМ СТАВИМ ОПЯТЬ НЕ ШЛО ОТ ВАС НЕ ШЛО

СНОВА СТАВИМ СНОВА

c) When the reciprocal station gets out of phase (i.e. when the machines at both the transmitting and receiving ends are not running together). This likewise necessitates a repeat, [redacted]

(b)(1)
(b)(3)-P.L. 86-36

Reception of messages must be undertaken with the utmost care. It must not be interrupted, and above all the automatic starting switch (Dauerstart) must remain switched on without interruption. The key continues in phase during the longer pauses too. Any omission of cipher letters breaks the sequence of the key, [redacted] It is in any case advisable only to work on messages which have been perfectly received.

[redacted]

Ы В Т Ш І Ц М Ы Ч Я К Ц Ж Ю С К З Х К А Б Л Б Ю Д Ц Н І
Е Я Т Л Ц З Ы И Ь П Ж Ь Ж Б Е 4 Щ 9 У Ф Ч Ь С О Ч К П Л
Е Ь Ж П И З ; - + . ((8 [illegible] 5 Щ) Щ Й 2 + 8 Э Й 6
О І (, Щ [illegible] Э 4 [illegible] , 4 ([illegible] - [illegible] № З / Щ 5 [illegible] : = 5 Р
З В Н Ц У Ц У П Х Ч С Ф В Ч Ы Ц Ю Н О У Ч О Ц У З П К Е З Ь
Я Ш Ю Д Ф Ь : І П К М Ы Ц М [illegible] З 6 - 4 (; І . 2 = = З
7 % 9 2 0 + - / О К Ю Ы Р Ж І З Ц У В У М С А О Н А З О Ф
В Я Е В Д Р Р Г Е О Г Р С Х Ы С Ф Ш И Т

Clear Text:

Из Сейфа №312/31 2/16 14 7 43 Небо - Генерал Майору Козловскому - Откомандирован подполковник Жданов вашему личному распоряжению прибу дет 16 июля 1943года. Красин - № 312/31 2/16 14/7 Голубова

Ы В Т Ы Ч Ф Н Х Л Р Н З Ю Ш Ю Ж І Ь Ь Р Е К Ч О І Ч М Ц Ь З
Ш Л Ж Т Т І О В Ф І Ь В Х С М В Ю Ю У Ф М Ю [illegible] Х Б А Е
Ю Ь П Р К Ю %) [illegible] [illegible] № / Й : = 5 Щ 0 4 5 8 З : 8 М
Л М О Е Щ ? ? = [illegible] 5 [illegible] 8 Э . 8 З № Й [illegible] Щ О І Б Щ Ф
В Д Ш Я П Ц Я И Э , 7 : = Щ / : 8 : 8 4 Е Ч Ш Я П
Ч Ж Д ! ! 7 : І ? Э З О / = 5 7 : - =; , ! (9 , [illegible] Й 7 .
. ; = ? Э З = 4 Щ О І : 5 [illegible] 2 Щ (З [illegible] ! + Й / О Э) : -
З 2 К Ч Ш Р Р Н Н П Щ 9 № / Щ [illegible] / 9 - [illegible] % - Й - [illegible] Э
/ 6 6 - № + Щ (. 8 4) ; Э + Щ Э 7 !)

Clear Text:

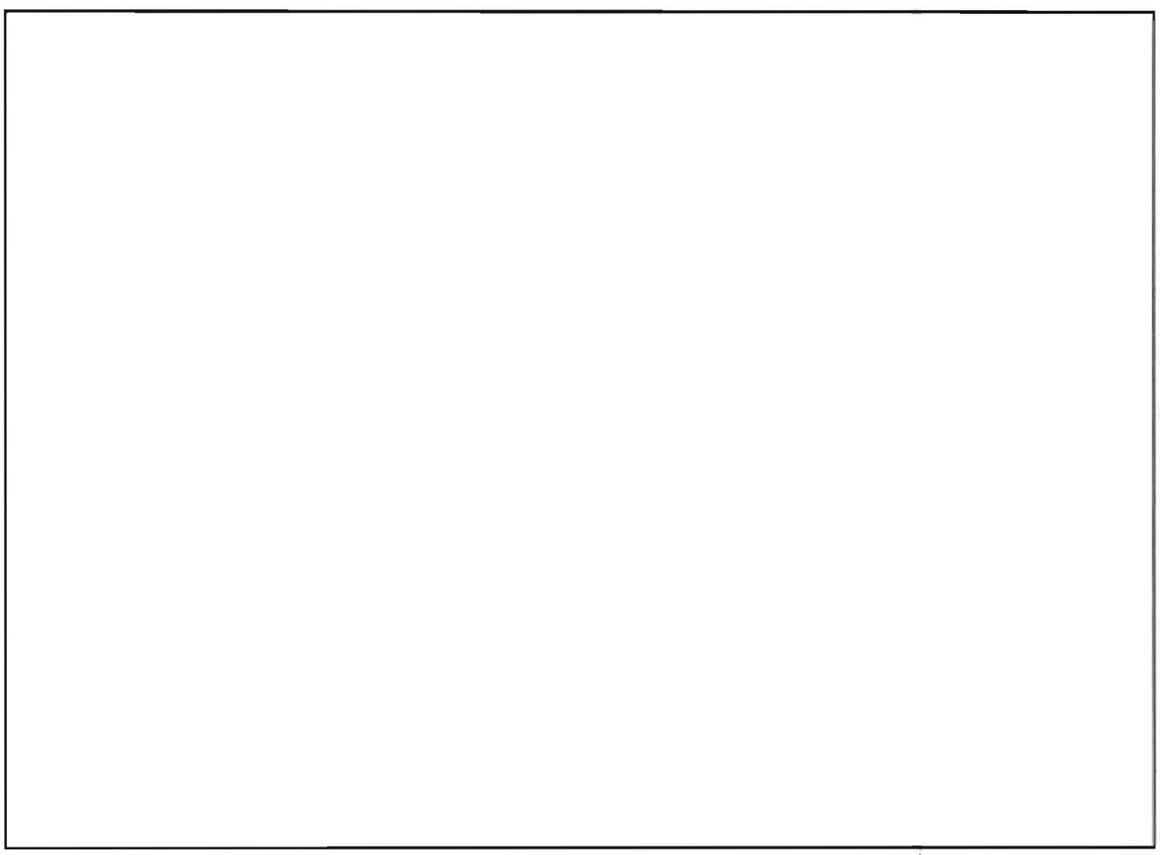
Из Сейфа 316/31 4/23 14/7/43 Небо - Генералу Прокофьеву- Аппараты с улучшенной экранировкой высланы 12/7 проверить имеющиеся в работе и дать точный отчет о их работе и обнаруженных дефектах Кашин - № 316/31 4/16 14/7 - Голубова 2047

Errors cancelled by using the figure shift (V) of ЩЩ . Thus in cancellation 4 ЩЩ ... would be enciphered.

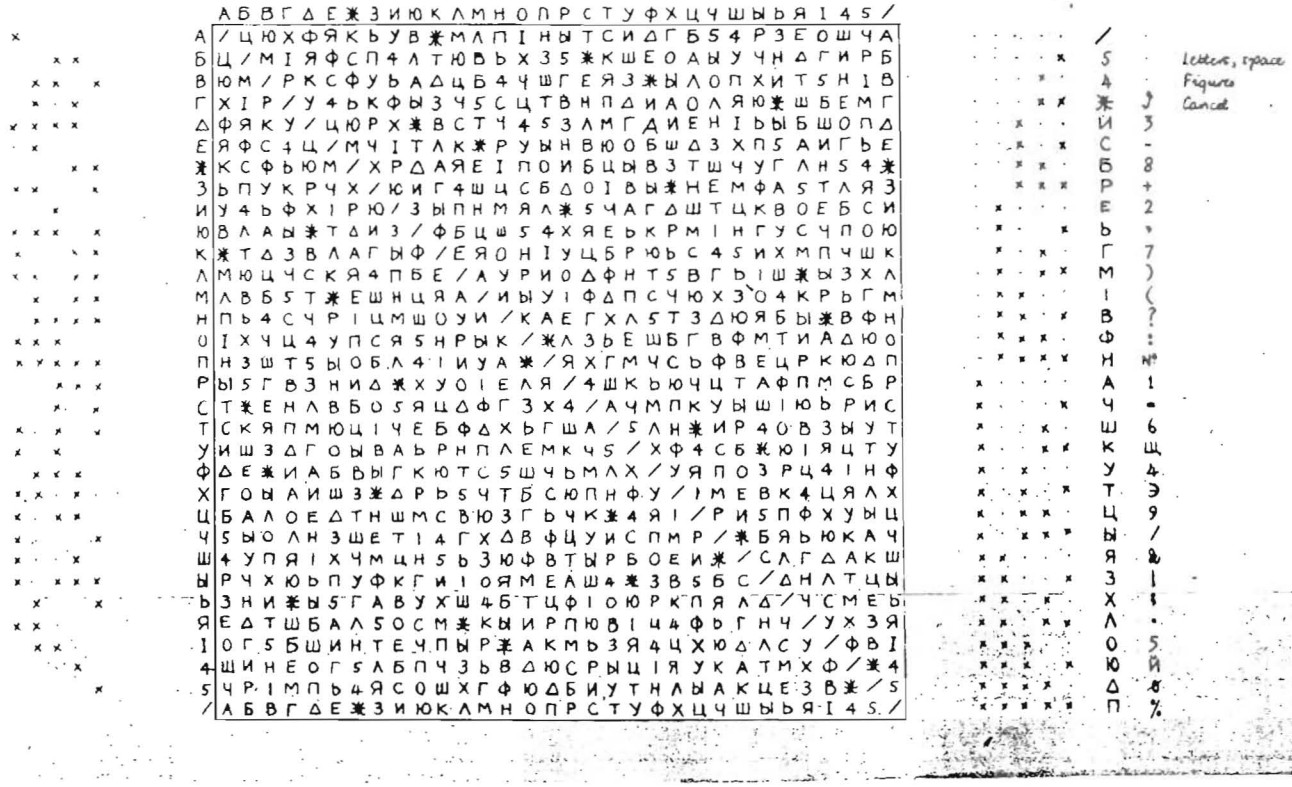
In the example given, the final group 4/16 is wrong - the last groups must be repeated:

жжж № 316/31 4/13 14/7/43 - Голубова 2047

(b)(1)
(b)(3)-P.L. 86-36



DOCID: 3283567



Pages 8 -24 redacted

1) Recce reports

a) Reports from Front HQ's to GHQ. Statements on own positions and situation, enemy situation, statements by P/W's, Sigint reports.

b) Summarized reports for general information of Front HQ's issued by G.H.Q. Moscow.

c) Reports for TASS and SOVINFORMBUREAU from Front HQ's or from war correspondents. Front line reports of every kind.

2) Reports and orders regarding the signals network of GHQ and the Front HQ's.

3) Letters between the personnel section of GHQ and the personnel sections of the Front HQ's, concerning postings, transfers, promotions etc.

4) Messages dealing with supplies. Rear area services' traffic.

5) Met service. Weather situation and forecasts.

On the air forces' network:

1) Meteorological service.

2) Communications of the section dealing with rear area services (supplies, personnel matters).